NIST Special Publication 800-39

Managing Risk from Information Systems

An Organizational Perspective

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than classified national security information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-39, 51 pages

(October 2007) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT IS OCTOBER 29-DECEMBER 14, 2007.
COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY
LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgements

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, and Gary Stoneburner wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. In another collaboration initiative, NIST is working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Notes to Reviewers

NIST Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, is the flagship document in the series of FISMA-related security standards and guidelines developed by NIST. This publication describes the NIST Risk Management Framework and provides guidance on a variety of important information security issues including:

- Organization-wide perspectives on managing risk from information systems;
- Risk-based protection strategies;
- Trustworthiness of information systems and trust relationships among organizations;
- Managing risk from external providers of services and information;
- Strategic considerations for managing risk related to the operation and use of information systems; and
- Use of the risk executive function.

In addition to the above issues, Special Publication 800-39 provides information on applying the steps of the Risk Management Framework to the phases of the system development life cycle to help ensure that information security is tightly integrated into the mission and business functions of organizations.

The material is this draft publication benefited from the close collaboration and cooperation with the Office of the Director of National Intelligence and the Department of Defense as part of the ongoing transformation initiative that is fostering convergence on key information security standards and guidelines across the federal government. The unified framework resulting from these activities will provide the Civil, Defense, and Intelligence Communities a standardized approach for achieving information security building on a common foundation of best practices while allowing communities of interest to define unique security requirements as the need arises.

The development of Special Publication 800-39 is the first step in a two-step process to redesign the NIST risk management guidelines. The current NIST recommendation on risk management, Special Publication 800-30, is being revised to focus exclusively on risk assessments as applied to the various steps in the Risk Management Framework described in Special Publication 800-39. The initial draft of Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, is projected for publication in January 2008.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors continue to help shape our publications and ensure that they are meeting the needs of our customers.

-- RON ROSS
FISMA IMPLEMENTATION PROJECT LEADER

Table of Contents

Prologue

"…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

CHAPTER ONE

INTRODUCTION

THE NEED FOR MANAGING ORGANIZATIONAL RISK FROM INFORMATION SYSTEMS

Information technology is widely recognized as the engine that drives the U.S. economy, giving industry a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizations[3] in the public and private sectors depend on information technology and the information systems[4] that are developed from that technology to successfully carry out their missions and business functions. Information systems are subject to serious *threats* that can have adverse effects on organizational operations (including missions, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. Threats to information systems include environmental disruptions, human errors, and purposeful attacks by hostile entities such as nation states, terrorist groups, hackers, criminals, and disgruntled employees. Given the significant danger of these types of threats, it is imperative that senior leaders understand their responsibilities in managing the risks from information systems that support the missions and business functions of the organization. Attacks on information systems[5] today are often well organized, disciplined, aggressive, well funded, and in a growing number of documented cases, extremely sophisticated. Successful attacks on public and private sector information systems can result in unauthorized disclosure or modification of highly sensitive information or a mission impacting denial of service.

Risk management recognizes that organizations operate in a highly complex and interconnected world using state-of-the-art information systems—systems that organizations depend upon to accomplish their missions and to carry out their business functions. Risk management also recognizes that explicit, management decisions are necessary in order to balance the benefits gained from use of these information systems with the risk of these same systems being the vehicle through which adversaries cause mission or business failure. Managing risk is not an exact science. It brings together the best collective judgments of the individuals responsible for the strategic planning and day-to-day operations of organizations to provide adequate security[6] for the information systems supporting the critical missions and business functions of those organizations. Risk related to information systems is just another component of organizational risk[7] that senior leaders address as a routine part of their ongoing management responsibilities.

[3] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements) that is charged with carrying out assigned missions and business functions and that uses information systems in support of those missions and business functions.

[4] An information system is a discrete set of information resources (people, processes, and technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[5] Attacks on information systems consist of specific actions taken by adversaries to cause harm to organizational operations, organizational assets, individuals, other organizations, or the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems.

[6] The Office of Management and Budget (OMB) Circular A-130, Appendix III, describes adequate security as security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

[7] Organizational risk includes many types of risk, for example, program management risk (e.g., cost, schedule, and performance risk), supply chain risk, budgetary risk, legal liability risk, safety risk, and inventory risk.

Managing that portion of organizational risk related to information systems begins with an effective information security program. The E-Government Act of 2002 (Public Law 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, known as the Federal Information Security Management Act (FISMA), states that an effective information security program includes:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and address information security throughout the life cycle of each organizational information system;
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

For risks related to information systems, a fundamental commitment is essential on the part of the senior leadership of the organization to make information security a first-order mission/business requirement. This commitment ensures that sufficient resources are available in the design, development, implementation, operation, and disposition of information systems to provide adequate levels of security for the systems in light of the explicit expectations being placed upon those systems. Information security should be considered a strategic capability and an enabler of missions and business functions across the organization. Information security is one important factor, among many, that should be considered by senior leaders in carrying out their responsibilities within the organization.

Since mission and business success depends on information systems, those systems must be dependable. To be dependable in the face of sophisticated 21st century threats, the systems must be adequately protected and used wisely.

1.1 PURPOSE AND APPLICABILITY

The purpose of NIST Special Publication 800-39 is to provide guidelines for managing risk to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of information systems. Special Publication 800-39 is the flagship document in the series of FISMA-related publications developed by NIST and provides a disciplined, structured, flexible, extensible, and repeatable approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of the organization. The risk management concepts described in this publication are intentionally broad-based, with the specific details of assessing risk and employing appropriate risk mitigation strategies provided by supporting NIST security standards and guidelines.[8] The guidelines are applicable to all federal information systems[9] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542[10] and are consistent with the risk management approaches and associated activities defined in the Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP).[11] In addition to the agencies of the federal government, state, local, and tribal governments and private sector organizations that are part of the critical infrastructure of the United States, are encouraged to use these risk management guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience within organizations including:

- Individuals with mission/business/information ownership responsibilities (e.g., agency heads, information owners, authorizing officials[12]);
- Individuals with information system/security management responsibilities (e.g., chief information officers, senior agency information security officers);
- Individuals with information system design and development responsibilities (e.g., program managers, information system integrators);
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, system administrators, system security officers); and
- Individuals with information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents).

[8] The NIST *Risk Management Framework* described in Chapter Three of this publication provides references to the specific security standards and guidelines needed to carry out effective risk management programs including the conduct of risk assessments and the selection and employment of appropriate safeguards and countermeasures to provide adequate protection for organizational missions and business functions.

[9] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[10] NIST Special Publication 800-59 provides guidance on identifying information systems as national security systems. The Director of National Intelligence (DNI) provides guidance to the Intelligence Community regarding the use of NIST publications for classified national security information and national security systems.

[11] Appendix E provides additional information on risk management activities in the NIPP.

[12] Authorizing officials are officials within an organization with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Authorizing officials are accountable for their authorization decisions.

1.3 RELATIONSHIP TO OTHER INFORMATION SECURITY PUBLICATIONS

The Risk Management Framework described in this publication integrates all of the security standards and guidelines necessary for building and implementing a technically sound and operationally effective information security program within an organization. Specifically, the framework provides key linkages among the following publications:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*;
- NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*;[13]
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*;
- NIST Special Publication 800-53A (Draft), *Guide for Assessing the Security Controls in Federal Information Systems*;
- NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

Special Publication 800-39 also incorporates many of the important information security concepts described in other NIST publications including, for example, Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, and Special Publication 800-100, *Information Security Handbook: A Guide for Managers.*

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes some of the fundamental concepts associated with managing risk from the operation and use of information systems including: (i) an organization-wide perspective for employing information security; (ii) the application of risk-based protection strategies in selecting and implementing effective safeguards and countermeasures for information systems; (iii) key factors in defining trustworthiness of information systems; (iv) the essential actions for establishing trust relationships among organizations; and (v) planning considerations for employing a defense-in-breadth protection strategy.

[13] NIST Special Publication 800-39 and an upcoming revision to Special Publication 800-30 represent a two-step process to revising the NIST risk management guidelines. The current NIST recommendation on risk management, Special Publication 800-30, is being revised to focus exclusively on risk assessments as applied to the various steps in the Risk Management Framework described in Special Publication 800-39.

- **Chapter Three** describes the process of applying the NIST Risk Management Framework to information systems across an organization including: (i) categorizing information systems with regard to mission and business impacts; (ii) selecting and tailoring minimum baseline security controls (i.e., specifying necessary risk mitigation); (iii) supplementing tailored security control baselines based upon risk assessments (i.e., specifying sufficient risk mitigation); (iv) documenting security controls and risk management decisions in system security plans; (v) implementing security controls in information systems (i.e., employing agreed-upon risk mitigation); (vi) assessing security controls to determine effectiveness (i.e., verifying risk mitigation effectiveness); (vii) authorizing information systems and explicitly accepting mission/business risk; and (viii) ongoing monitoring of the security state of information systems, information security programs, and operational environments.
- **Supporting appendices** provide additional risk management-related information including: (i) references; (ii) terms and definitions; (iii) acronyms; (iv) integrating risk management concepts into the acquisition and system development life cycle processes; and (v) mapping the NIST Risk Management Framework to the framework for risk management in the National Infrastructure Protection Plan.

CHAPTER TWO

THE FUNDAMENTALS

ORGANIZATIONAL RISK MANAGEMENT, ESTABLISHING TRUST, AND DEFENSE-IN-BREADTH

This chapter describes some of the fundamental issues associated with managing risk from information systems including: (i) the advantages of developing and implementing an organization-wide information security program; (ii) the use of risk-based protection strategies to achieve adequate protection for the organization's missions and business functions; (iii) the factors that define trustworthiness of information systems; (iv) the essential actions for establishing trust relationships among organizations and partners; and (v) planning considerations for employing a defense-in-breath protection strategy.

2.1 ORGANIZATION-WIDE PERSPECTIVE

The complexity and diversity of missions and business functions in modern organizations and the multitude of information systems that support those missions and business functions demand an organization-wide approach to managing information security and the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation. Developing a comprehensive organization-wide information security program is not a new concept. However, obtaining an organization-wide perspective by all authorizing officials and senior leaders provides a new and more comprehensive view of managing organizational risk resulting from the operation and use of information systems. In today's organizations, a single mission or business function may be supported by multiple information systems. Conversely, there may be multiple complex missions and business functions across the organization that are supported by a single information system. This many-to-many relationship among missions/business functions and systems suggests an organization-wide approach to implementing information security and managing risk. There are many advantages to employing an organizational approach when building a security program for the organization's information systems.[14] An organization-wide information security program:

- Facilitates prioritization of information security requirements and allocation of information security resources based on impact to the organization's missions/business functions;
- Ensures information security considerations are integrated into the Federal Enterprise Architecture, the programming, planning, and budgeting cycles for managing information system assets, and the acquisition/system development life cycles;
- Promotes the development and dissemination of common information security policies and procedures;
- Promotes the identification, development, implementation, and assessment of common (infrastructure-based) security controls that support large segments of the organization;
- Provides insights into systemic information security weaknesses and deficiencies;
- Promotes the development of organization-wide solutions to information security problems and more consistent and cost-effective information security solutions;
- Facilitates decisions on risk mitigation activities based on organizational priorities;

[14] OMB Circular A-130 and NIST Special Publication 800-100 provide guidance on organization-wide information security programs.

- Promotes better communication among personnel responsible for information security;
- Increases the information security knowledge base for key individuals responsible for protecting organizational missions and business functions; and
- Provides an essential foundation for building trust among organizations/partners.

To be effective, organization-wide information security programs require the strong commitment, direct involvement, and ongoing support from senior leaders. The objective is to *institutionalize* information security into the infrastructure of the organization to ensure that the protection of missions and business functions is always a priority and an integral part of how the organization conducts its operations in cyberspace.

Incorporating Information Security into Enterprise Architectures

Enterprise architectures provide a common language for discussing information security in the context of missions/business functions and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activity boundaries. For the federal government, the Federal Enterprise Architecture defines a collection of interrelated reference models that are focused on lines of business including Performance, Business, Service Component, Data, and Technical and a security and privacy profile that describes how to integrate information security requirements into the reference models. The Federal Enterprise Architecture Security and Privacy Profile is a scalable and repeatable methodology for addressing information security and privacy from a business-centric and operational perspective. The profile integrates the disparate perspectives of program, security, privacy, and capital planning into a coherent process, using an organization's enterprise architecture efforts.

The Federal Enterprise Architecture Security and Privacy Profile adapts the reference models for use in describing information security and privacy considerations and provides the necessary linkage from enterprise architectures to the NIST security standards and guidelines that are used to implement the needed safeguards and countermeasures within federal information systems.[15] For example, a particular line of business may achieve its mission or business objectives by using a variety of information systems within the organization. The organization would first use FIPS 199 to determine the potential impact on each specified line of business due to a loss of confidentiality, integrity, or availability in the supporting information systems. It may be necessary to decompose the lines of business further into sub-function and process levels to achieve the necessary details to engage the mission/business process owners and partners in determining other specific elements of risk. This additional information will allow responsible and accountable officials to make informed risk-based decisions to drive the selection of appropriate security and privacy controls.

Integrating Information Security into the System Development Life Cycle

In addition to using enterprise architectures to guide information security decisions, information security-related activities should be fully integrated into the system development life cycles for information systems.[16] Information security activities take place at every phase in the system

[15] Chapter Three describes the NIST Risk Management Framework and provides additional guidance on the allocation of specific safeguards and countermeasures (i.e., security controls) to components of information systems that are defined by enterprise architectures.

[16] There are five phases in the system development life cycle: (i) system initiation; (ii) system development and acquisition; (iii) system implementation; (iv) system operations and maintenance; and (v) system disposition (disposal).

development life cycle.[17] For example, it is important that the organization define and incorporate information security requirements into the initial design and development of the information system during the initiation and development/acquisition phases of the system development life cycle.[18] The information security requirements define the needed security functionality,[19] the quality of the functionality, and the assurance (i.e., grounds for confidence) that the required functionality and quality are obtained (see related definition of trustworthiness of information systems in Section 2.3). The implementation phase of the life cycle provides an opportunity to determine the effectiveness of the security controls that have been employed within the information system prior to the commencement of actual operations. Once approved for operation, the information system moves into the operations and maintenance phase of the life cycle where continuous monitoring of implemented security controls and the operational environment helps ensure that missions and business functions are protected on an ongoing basis. During the disposition phase of the life cycle, the organization ensures that critical or sensitive information that may cause adverse impacts, if compromised, is verifiably removed from system components prior to disposal.

Many of the routine activities conducted during the system development life cycle can support or are complementary to the information security activities that are required to be carried out by the organization. Organizations should maximize the use of relevant information, evidence, and artifacts generated during the system development life cycle to satisfy requirements for similar information, evidence, and artifacts needed for information security purposes—thus eliminating unnecessary repetition, cost, and documentation that may result when security activities are conducted independently of routine system life cycle processes. Organizations should ensure that there is close collaboration and cooperation among personnel responsible for the design, development, implementation, operation, and disposition of organizational information systems and the information security professionals advising the senior leadership on appropriate safeguards and countermeasures (i.e., security controls) needed to adequately mitigate risk and protect critical missions and business functions. A tight coupling of information security-related activities and requirements into the system development life cycle ensures that senior leaders consider the specific risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the use of information systems and take appropriate actions to carry out the organization's security due diligence.

An effective organization-wide information security program helps to ensure that security considerations are addressed in the enterprise architecture for the organization and integrated into the system development life cycle.

[17] NIST Special Publications 800-64 and 800-100 provide guidance on integrating information security activities into the specific phases of the system development life cycle. Appendix D provides additional information on incorporating the steps in the NIST Risk Management Framework (described in Chapter Three) into the system development life cycle phases.

[18] Information security requirements are defined in FIPS 200, NIST Special Publication 800-53, and other FISMA-related information security standards and guidelines.

[19] Security functionality is the set of management, operational, and technical security controls within an information system implemented by a combination of people, processes, and technologies. Security controls are described in NIST Special Publication 800-53.

Risk Executive Function

Many approaches to managing information security and risk today focus on individual information systems and the authorization decisions associated with those systems without adequate regard to the complex relationships among the missions and business functions carried out by the organization. Authorizing officials, in many cases, may have a very narrow or localized perspective in rendering authorization decisions, perhaps without fully understanding or explicitly accepting the risk incurred by the organization in making such decisions.[20] Organizations need a holistic approach for addressing risk—an approach that provides greater visibility into the integrated operations/business flows of the organization.

To address the issues related to mission and business process risk and the associated information security capabilities that must be in place to achieve adequate protection, organizations should consider including management of organizational risks from information systems as part of an overall a *risk executive* function.[21] A risk executive function helps ensure that information security considerations for individual information systems to include the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall goals and objectives of the organization in carrying out its critical missions and business functions. The risk executive function provides *visibility* into the individual decisions of authorizing officials and provides a holistic view of risk to the organization beyond that risk associated with the operation and use of information systems. While authorizing officials are, by definition, senior leaders with mission/business process ownership and budgetary responsibilities, it is possible or even likely that their authorization decisions may affect, either directly or indirectly, other parts of the organization supported by their information systems. In contrast, it is also possible that multiple authorizing officials may be responsible for information systems which collectively support a single organizational mission or business process. A risk executive function facilitates the sharing of security-related and risk-related information[22] among authorizing officials and other senior leaders within the organization to consider all types of risks that may affect mission/business success and the overall interests of the organization at large.

In addition to the aforementioned internal authorization decisions, there is also increasing reliance on external providers to provide important information system/security services and information that the organization depends on to carry out its critical missions and business functions. A risk

[20] Authorizing officials are officials within an organization with the authority to formally approve the operation of an information system. The original responsibility of authorizing officials published in FIPS 200 and NIST Special Publication 800-37 (authorization with regard to risks to the organization, to its assets, and to individuals) was extended in NIST Special Publication 800-53 (i.e., through security control RA-2) to address risks to other organizations and to the Nation.

[21] The risk executive function is not limited to addressing risks resulting from information systems, although that is the focus for the discussion in this document. A risk executive function does not presume any type of formal organizational structure or formal responsibility assigned to any individual or group within the organization. Organizations have flexibility in how the risk executive function is implemented. For the federal government, the risk executive function may be delegated by the agency head to another organizational official (e.g., the Chief Information Officer). In situations where the risk executive function is delegated to an organizational official who has independent responsibilities for authorizing one or more information systems that can affect the missions and business functions supported by other authorizing officials, the head of the agency should provide the function to ensure impartiality and that organizational risk is adequately addressed.

[22] For example, FIPS 199 impact analyses for individual information systems may be conducted as an organization-wide activity and the resulting security categorizations shared with authorizing officials and other senior leaders within the organization. The selection of common security controls for the organization may also be conducted as an organization-wide activity and the resulting information regarding assignments of responsibility for common security control development, implementation, and assessment shared among appropriate organizational personnel.

executive function helps to ensure that the shared responsibility for supporting organization-wide missions and business functions using external providers receives the needed visibility and is elevated to the appropriate decision-making authorities. The additional potential risk assumed by the organization through the use of external providers of services and information can be brought forward by the risk executive function and considered along with other organizational risks.

In general, managing organizational risks from information systems as part of an overall risk executive function:

- Provides senior leadership oversight for all information security activities across the organization including the allocation of resources and explicit risk acceptance decisions;
- Ensures individual authorization decisions by authorizing officials consider all factors necessary for mission and business success organization-wide;
- Provides an organization-wide forum to consider all sources of risks to organizational operations, organizational assets, individuals, other organizations, and the Nation;
- Promotes cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility; and
- Ensures that information security activities that have organization-wide effects are managed by and coordinated with appropriate organizational entities.

Figure 1 illustrates the relationships among authorizing officials, the information systems that support organizational missions and business functions, and the risk executive function.[23]

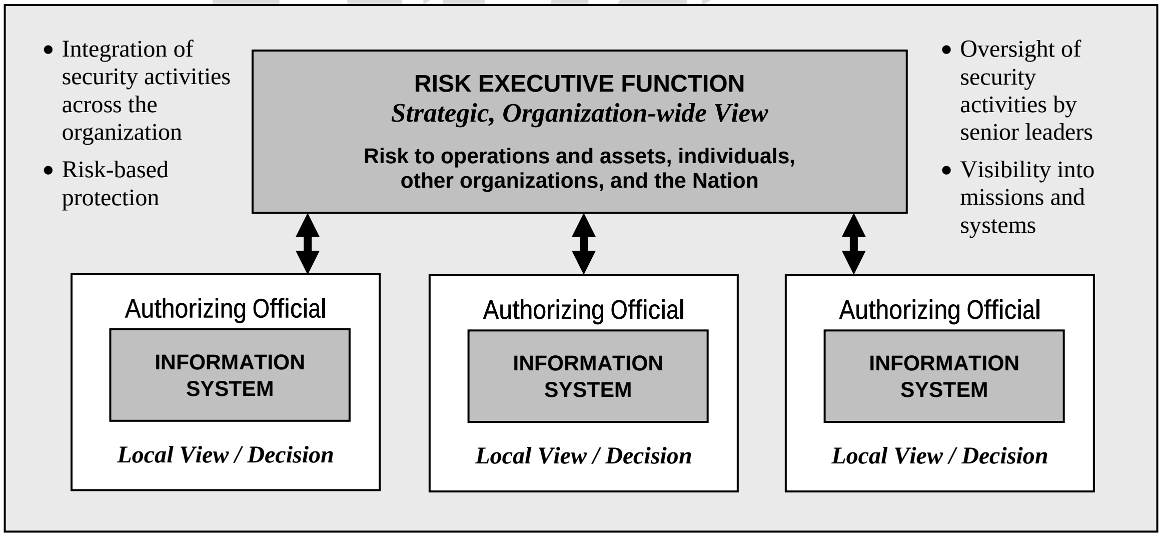
• Integration of security activities across the organization
• Risk-based protection
RISK EXECUTIVE FUNCTION
Strategic, Organization-wide View
Risk to operations and assets, individuals, other organizations, and the Nation
• Oversight of security activities by senior leaders
• Visibility into missions and systems
Authorizing Official
INFORMATION SYSTEM
Local View / Decision
Authorizing Official
INFORMATION SYSTEM
Local View / Decision
Authorizing Official
INFORMATION SYSTEM
Local View / Decision

FIGURE 1. RISK EXECUTIVE FUNCTION

[23] NIST Special Publication 800-100 provides guidance on program-level information security issues to include some of the activities associated with a risk executive function.

2.2 RISK-BASED PROTECTION STRATEGIES

To protect organizations from the adverse effects of ongoing, serious, and increasingly sophisticated *threats*, organizations should focus on risk-based protection. Risk-based protection strategies are characterized by explicitly identifying, mitigating as deemed appropriate, and accepting the resulting risks associated with the use of information systems in carrying out organizational missions and business functions. Risk-based protection strategies require authorizing officials to: (i) determine the appropriate balance between the risks from and the benefits of using information systems in carrying out their organizational missions and business functions; (ii) carefully select, tailor, and supplement the safeguards and countermeasures (i.e., security controls) for information systems necessary to achieve this balance; (iii) take responsibility for the information security solutions agreed upon and implemented within the information systems supporting the organization; (iv) fully acknowledge and explicitly accept the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation that result from the operation and use of information systems to support the organization's missions and business functions; and (v) be accountable for the results of their information security-related decisions. Risk-based protection strategies focus on managing risks from information systems based on real-world conditions and making the management decisions explicit—an essential requirement for establishing and maintaining trust among organizations (as further discussed in Section 2.4).

Risk-based protection strategies are necessary to help ensure that organizations are adequately protected against the growing sophistication of threats to information systems. The serious nature of the threats along with the dynamic environment in which modern organizations operate, demand flexible, scalable, and mobile defenses that can be tailored to rapidly changing conditions including the emergence of new threats, vulnerabilities, and technologies. Risk-based protection strategies support the overall goals and objectives of organizations, can be tightly coupled to enterprise architectures, and operate within system development life cycles. By empowering senior leaders to make explicit risk management decisions, these strategies also enable the flexibility necessary for the selection and employment of the right set of security controls at the right time to achieve commonsense, cost-effective information security solutions. The NIST Risk Management Framework described in Chapter Three supports risk-based protection by providing a disciplined, structured, flexible, extensible, and repeatable approach to building information security programs and managing risks associated with the ongoing operation and use of information systems.

Explicit statements of the risks to the organization being accepted by authorizing officials (reflecting an organization's risk tolerance) is the foundation of risk-based protection and is essential for establishing trust relationships among organizations. The implicit risk acceptance associated with other protection strategies hides the degree of risk being accepted, thereby inhibiting the trust relationships among organizations that are essential for an environment of information sharing.

2.3 TRUSTWORTHINESS OF INFORMATION SYSTEMS

The concept of *trustworthiness* is an important consideration for senior leaders in making credible, risk-based decisions regarding the development, implementation, operation, and disposition of information systems and the potential impact those systems may have on organizational missions and business functions. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthiness defines the security state of the information system at a particular point in time and is measurable. Trustworthy information systems are systems that are worthy of being trusted to operate within defined levels of *risk* to organizational operations, organizational assets, individuals, other organizations, or the Nation, despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation.

There are several factors that can affect the trustworthiness of an information system including: (i) the *security functionality* (i.e., security-related functions or features) contained within the system; (ii) the *quality* of the design, development, implementation, and operation of the system (i.e., the degree to which the security functionality is correct, always invoked, non-bypassable, and resistant to tampering); and (iii) the *security assurance* of the system (i.e., the grounds for confidence that the claims made about the functionality and quality of the system are being met).[24] Security functionality can include, for example, identification and authentication mechanisms, access control mechanisms, auditing mechanisms, and encryption mechanisms. Quality can be addressed, for example, by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and good system/security engineering principles and concepts when building information technology components and when composing information systems from those components. Security assurance can be obtained from a variety of sources including, but not limited to, evidence brought forward regarding the design, development, implementation, and operation of the information system, the results of independent assessments (e.g., analyses, testing, evaluation, inspections, and audits) of the system conducted by qualified assessors, and the results of security incident reporting.

Understanding trustworthiness is important to ensuring that information systems are able to provide an appropriate degree of protection should there be a breach in the systems and a loss of confidentiality, integrity, or availability.[25] Information systems with a higher degree of trustworthiness are expected to exhibit a higher degree of penetration resistance against a wide range of adversaries with varying degrees of sophistication in the attacks employed. The operational environment and the maximum acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, or the Nation guide the degree of trustworthiness needed.

[24] Functionality, quality, and assurance requirements are described in NIST Special Publication 800-53. Security functionality is provided by the management, operational, and technical security controls in Appendix F, the security controls catalog. Security assurance and quality considerations are addressed in Appendix E, minimum assurance requirements.

[25] The concept of trustworthiness is independent of the concept of impact levels described in FIPS 199. The degree of trustworthiness of an information system, when viewed against the worst-case impact analysis and the associated impact levels in FIPS 199, determines the ultimate risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. The baseline security controls along with the tailoring and supplementation guidance described in NIST Special Publication 800-53, provide a flexible approach for ensuring that the degree of trustworthiness of an information system is commensurate with the system impact level.

2.4 ESTABLISHING TRUST RELATIONSHIPS AMONG ORGANIZATIONS

The need for *trust relationships* among organizations arises both from an organization's use of external providers of information system services and from partnerships established to share information and conduct business.[26] The former has the general relationship of customer/provider while the latter is more of a peer-to-peer relationship. Organizations are becoming increasingly reliant on information system services[27] and information provided by external providers to carry out important missions and business functions. In many cases, the service providers bring greater productivity and cost efficiencies to the organization in carrying out its missions and business functions. Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain[28] exchanges (i.e., supply chain collaborations or partnerships). The growing dependence on external service providers and the relationships being forged with those providers present new challenges for organizations, especially in the area of information security. These challenges include, for example: (i) defining the types of services and information provided to the organization; (ii) describing how the services and information are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation resulting from the use of the services or information, is at an acceptable level.

The assurance (i.e., grounds for confidence) that the organizational risk is at an acceptable level depends, in part, on the trust relationships established among organizations.[29] While the specifics of establishing trust differ for customer/provider and peer-to-peer relationships, trust cannot be conferred upon providers or partners, it must be earned. Trust is earned by the prospective providers or partners:

- Identifying the common goals and objectives for the provision of services/information or information sharing;
- Agreeing upon the risk associated with the provision of such services or information sharing;
- Agreeing upon the degree of trustworthiness needed for the information systems processing, storing, or transmitting shared information or providing services in order to adequately mitigate the risk;
- Determining if the information systems are worthy of being trusted to operate within the agreed-upon levels of risk despite environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation; and
- Providing ongoing monitoring and oversight to ensure that the trust relationship is being maintained.

[26] Trust relationships can be either inter-organizational or intra-organizational in nature.

[27] External information system services are services that are implemented outside of the system's traditional authorization boundary (i.e., services that are used by, but not a part of, the organizational information system).

[28] Supply chain refers to the distribution channel of a product from its sourcing to its delivery to the end consumer.

[29] The level of trust that an organization places in an external service provider or mission/business partner can vary widely ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector). External service providers can be either public or private sector entities.

Trust relationships among participating/cooperating partners depend on carrying out each of the five elements of trust described above. The objective is to achieve an *understanding* of the prospective partner's information security programs and information systems in order to establish an environment conducive to information sharing or to obtaining information system services.[30] Trust relationships depend on the *actions* taken by the participating/cooperating partners to agree upon and provide the appropriate safeguards and countermeasures for the information systems supporting the partnerships and the *evidence* produced by the partnering organizations demonstrating that the agreed upon safeguards and countermeasures have been implemented as intended. This evidence can include documents such as information system security plans (including risk assessments), security assessment reports, and plans of actions and milestones. Figure 2 illustrates the types of evidence that can be used to support the establishment of trust relationships among partners.

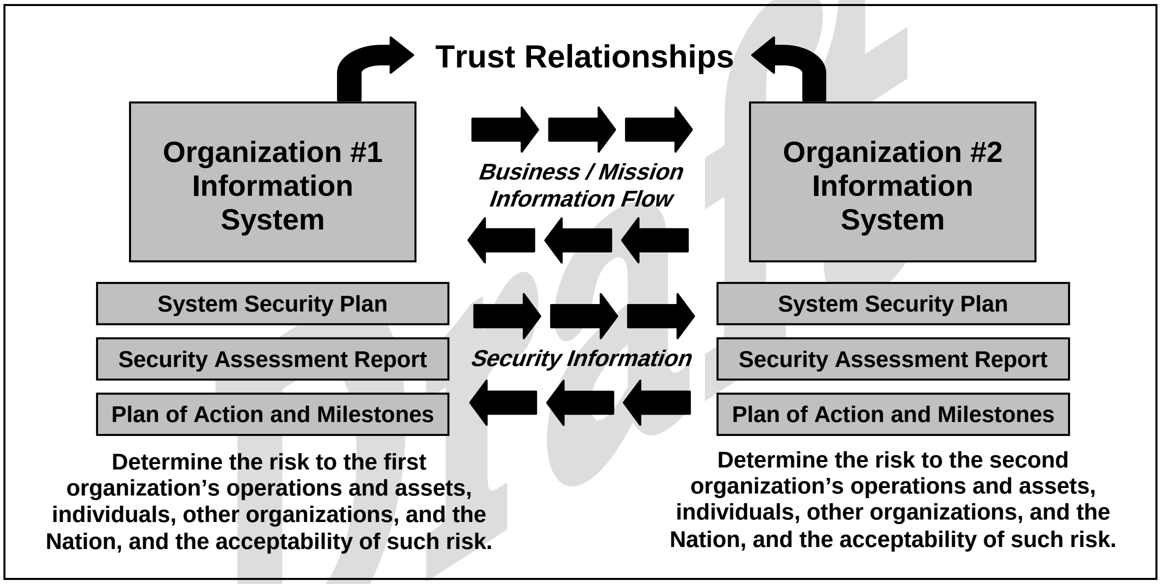
Trust Relationships
Organization #1 Information System
Business / Mission Information Flow
Organization #2 Information System
System Security Plan
Security Assessment Report
Plan of Action and Milestones
Security Information
System Security Plan
Security Assessment Report
Plan of Action and Milestones
Determine the risk to the first organization's operations and assets, individuals, other organizations, and the Nation, and the acceptability of such risk.
Determine the risk to the second organization's operations and assets, individuals, other organizations, and the Nation, and the acceptability of such risk.

FIGURE 2: BUILDING TRUST RELATIONSHIPS AMONG PARTNERS

An example of an inter-organization trust relationship for shared service providers is provided in the application of the Federal Public Key Infrastructure (PKI) Policy Authority. The Federal Public Key Infrastructure (PKI) Policy Authority established a compliance audit process that provides a basis for federal agencies to trust each others' digital certificates, and for federal agencies and cross-certified nonfederal PKIs to trust digital certificates issued by each others PKIs at known and verified levels of assurance. These trust relationships were established by carrying out the five elements of trust described above. Initially, the Federal PKI Policy Authority and the prospective providers of digital certificates agreed upon the PKI services that were to be provided. Next, the Federal PKI Policy Authority and the prospective PKI service providers agreed upon the level of risk in providing such services and the necessary safeguards

[30] Trust is subjective with no precise formula for combining and balancing the various elements of trust. The model offered here for establishing trust among organizations identifies those elements of trust essential for an effective dialogue in establishing trust relationships under mutually agreeable conditions and is not intended to require specific actions by organizations or prospective partners. This model provides organizations (i.e., prospective sharing partners or potential consumers of services/information from external providers) with a common process for coming to an agreement that a trustworthy environment has been established for the sharing of information or for the provision of services/information.

and countermeasures (i.e., security controls) that were needed to obtain assured PKI services. Then, for the Shared Service Provider Program that issues digital certificates on behalf of many federal agencies, the General Services Administration conducted a thorough assessment of the prospective providers' information systems that were to provide the PKI services, to ensure that the required safeguards and countermeasures were employed and effective in their application. Lastly, ongoing monitoring and oversight of all its trust relationships continues by the Federal PKI Policy Authority through the requirement for cross-certified PKIs and Shared Service Providers to submit the results of an annual, independent third-party audit of policies, procedures, and practices.

Ultimately, the responsibility for adequately mitigating risks to organizational operations, organizational assets, individuals, other organizations, or the Nation, resulting from the use of external services and information or partnering to conduct missions and business functions remains with the authorizing official. Authorizing officials should require that appropriate trust relationships be established with external providers and mission/business partners. For external providers and mission/business partners, a trust relationship[31] requires that the organization establish and retain a level of confidence that each participating provider or partner provides adequate protection for the services rendered or information shared.[32] The trust relationships can be very complicated due to the number of entities participating in the consumer-provider or partner relationship and the type of relationship between the parties.[33] External providers or partners may also, in turn, outsource the services to other external entities, making the trust relationships even more complicated and difficult to manage. Depending on the nature of the services provided or the information shared, it may be unwise for the organization to wholly trust the provider or partner—not due to any inherent untrustworthiness on the part of the other organization, but due to the intrinsic level of risk in using the services or the information. Where a sufficient level of trust cannot be established in the services, information, providers, or partners, the organization employs compensating controls or accepts the greater degree of risk to its missions and business functions.

[31] Trust in external providers is directly related to the trustworthiness of the provider's information systems. In practice, authorizing officials have varying degrees of information about the trustworthiness of provider's information systems. In some cases, the level of trust is based on the amount of direct control the authorizing official is able to exert on the provider with regard to the trustworthiness of the information systems, including the employment of appropriate safeguards and countermeasures necessary for the protection of the information or service and the evidence brought forth as to the effectiveness of those safeguards and countermeasures. The degree of control is, in most cases, established by the terms and conditions of the contracts, service-level agreements, or interagency agreements with the external service providers and can range from extensive (e.g., negotiating a specific contract or agreement that specifies detailed information security requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services such as commercial telecommunications services). In other cases, the level of trust is derived from other factors that convince the authorizing official that the requisite safeguards and countermeasures have been employed and that a credible determination of effectiveness exists.

[32] The provision of services by providers external to the organization may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, interagency agreements, etc.), the organization should develop such agreements and require the use of appropriate safeguards and countermeasures. When the organization is not in a position to require explicit agreements with external providers, the organization should make explicit any assumptions about the service capabilities with regard to security.

[33] The concept of a *trust relationship* is scaleable and can represent simple (bilateral) relationships among two partners or more complex many-to many relationships among many diverse partners.

2.5 STRATEGIC PLANNING CONSIDERATIONS

In order to effectively manage risks resulting from the operation and use of information systems to support organizational missions and business functions, senior leaders should consider issues that go beyond the trade-offs likely to be made within the context of individual system decisions. For example, in addition to the defense-in-depth approaches that are frequently used by organizations to allocate security controls within information systems to achieve layered defenses, other approaches should be considered in order to address issues such as supply chain concerns associated with the use of information technology products in organizational information systems. Uncertainty in the supply chain can make it very difficult to determine the trustworthiness of information systems which depend upon component information technology products to provide many of the safeguards and countermeasures necessary to ensure adequate security. Supply chain uncertainty and the growing sophistication of threats increase the potential for a range of adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation. To mitigate risk from supply chain issues, a comprehensive information security strategy should be considered that employs a strategic, organization-wide *defense-in-breadth* approach. The defense-in-breadth considerations include:

- Diversification of the portfolio of information technology assets within the organization;
- Management of the complexity of the information systems within the organization;
- Application of a balanced set of management, operational, and technical safeguards and countermeasures to organizational information systems to achieve defense-in-depth;
- Detection and response to breaches of information system boundaries;
- Restrictions on the use of information technologies based on the risks incurred by the deployment of such technologies; and
- Reengineering of organizational mission/business processes.

Diversification of Information Technology Assets

Driven by the desire to reduce operations and maintenance costs, promote interoperability, and increase usability, the federal government is moving towards an environment of organization-wide information technology infrastructures and applications. While such an approach provides sound economic and operational benefits, it can also create significant mission/business risk. Homogeneity in hardware and software components (typically commercial off-the-shelf products used to build information systems) can increase risk because the systems, networks, and interconnections within the information technology infrastructure of the organization can enable those with malicious intent to impact a greater number of organizational assets. Once an adversary is able to initiate a successful attack on an information system component, a similar attack can be successful on other components with less effort due to the homogeneity of the information technology and standard information system configurations. Diversifying the portfolio of information technology products used to build information systems presents differing targets for an adversary translating into greater difficulty in completing attacks that may debilitate an entire organization. The degree of information technology asset diversification should be commensurate with organizational risk.

Management of Information System Complexity

Information system complexity[34] generally increases mission and business risk. As the federal government moves toward greater homogeneity in its information technology components, it is also acquiring larger and more complex information systems that become significant targets of opportunity for adversaries. In addition to greater complexity resulting in increased opportunities for exploitation, successful attacks on large and complex information systems can result in single points of failure affecting significant segments of the organization and potentially increasing risk unless such systems are engineered to eliminate such single points of failure. Explicit efforts to manage complexity, for example, by partitioning information systems into smaller systems or subsystems can improve the information security posture of the organization.[35] A greater number of (smaller) information systems or subsystems presents attackers with a greater number of potential targets, but the success of any one attack is less likely to do severe or catastrophic damage to the organization's missions and business functions. Additionally, distributing information stored in systems across smaller systems or subsystems decreases the impact a successful attack would have on an organization. Organizations can implement a strategy of reducing target size by decreasing the complexity of information systems that support critical missions and business functions. The effort put forth in reducing the complexity of information systems should be commensurate with the risk to the organization.

Application of Balanced Safeguards and Countermeasures to Information Systems

Organizations should apply a balanced set of safeguards and countermeasures (i.e., management, operational, and technical security controls) to organizational information systems using a defense-in-depth strategy.[36] The objective is to provide multiple layers of protection and to reduce the number of information system vulnerabilities and the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation. Technical controls are obtained, in most cases, through the commercial marketplace when acquiring information technology products. Because of supply chain risks and the potential for malicious activity, there may be less assurance that the security controls implemented in information technology products are resilient in the face of serious threats, thus reducing the trustworthiness of the information systems where those products are employed. A reduction in the level of confidence in the technical security controls within organizational information systems may result in a greater reliance on management and operational controls that are less vulnerable to supply chain risks.

Detection and Response to Breaches of Information System Boundaries

Organizations should continue their security due diligence by regularly and methodically checking organizational information systems for breaches by adversaries. For extremely critical and sensitive information systems, organizations should assume that adversaries may have penetrated their defenses at some point and installed malicious code (e.g., worms, viruses, Trojan horses, rootkits, etc.) within the system boundary. Once inside the information system, intruders can do great damage to the organization by taking control of the system, compromising the confidentiality and integrity of the information processed, stored, and transmitted by the system, exfiltrating large quantities of information to hostile entities, and affecting the overall availability

[34] The size of an information system is an important factor in complexity.

[35] Partitioning information systems includes the concept of isolation or "air gapping" systems of significant impact to the organization in order to reduce the exposure of critical/sensitive information to adversaries through external network connections.

[36] NIST Special Publication 800-53 provides a breadth and depth of safeguards and countermeasures in the baseline security controls recommended for information systems in accordance with FIPS 199 impact levels.

of the system. These malicious activities can go virtually undetected by the organization unless specific detection and response strategies are employed and diligently followed. Detection strategies should include both network- and host-based intrusion detection and prevention programs that use signature, anomaly, and/or stateful analysis techniques.[37] Response strategies to malicious insiders should follow a few basic rules. Any information system suspected of being compromised and under the control of a malicious insider cannot be trusted to carry out any further functions, either diagnostic in nature or mission/business process-related. Sophisticated intruders can mask their activities and make it virtually impossible to detect ongoing malicious activities. The basic response strategies are containment, eradication, recovery, and application of lessons learned.[38] As with the other defense-in-breadth considerations, an organizational assessment of risk should guide any of the organization's activities in this area. Intrusions to organizational information systems should be reported to appropriate organizational officials.[39]

Consideration of Information Technology Use Restrictions

Even with diversification of information technology assets, reduction in the size and complexity of the information system, the application of a balanced set of security controls, and the application of detection and response strategies, the use of certain information technologies may introduce significant vulnerabilities into information systems that have the potential to increase risk beyond an acceptable level. Organizations should assess the risk to organizational operations and assets, individuals, other organizations, or the Nation that would result from the use of such technologies. If the organization cannot achieve the level of information system trustworthiness necessary to adequately reduce or mitigate the risk brought about by the introduction of those technologies, use restrictions may be needed. Information system use restrictions provide an alternative method to reduce or mitigate risk when, for example: (i) security controls cannot be implemented within the technology and/or resource constraints of the organization; or (ii) security controls lack reasonable expectation of effectiveness against identified threats. Careful consideration should be given to restricting how information technologies that introduce unacceptable risks are used by the organization.

Process Reengineering

Successfully managing the risk resulting from the operation and use of information systems may necessitate reengineering of the processes used to accomplish missions and execute business functions. While such reengineering efforts require significant commitment on the part of the organization, they are in line with the concepts incorporated in the OMB Federal Enterprise Architecture initiative—that is, the potential for risk is greatly influenced by decisions made in the definition of mission and business processes. These decisions include the manner and degree to which the organization relies upon information and exposes itself to harm through the use of information systems. By purposefully considering risk impacting decisions in the mission and business process definitions, there is the distinct potential for significant risk reduction within acceptable operational constraints. Conversely, failure to do so may well result in processes that impose undue risk that cannot be adequately mitigated with available resources. Therefore, avoiding unacceptable risk requires process decisions that are realistic with regard to risk tolerance and the trustworthiness of the information systems available within the organization's

[37] NIST Special Publication 800-94 provides guidance on intrusion diction and prevention systems.

[38] NIST Special Publication 800-83 provides guidance on malware incident prevention and handling.

[39] Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov in accordance with the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

resources. Unacceptable risk equates to the potential for mission or business failure, a state of affairs that is, by definition, not tolerable within organizations. The consideration of process reengineering is, with the currently available information technology, likely to be an important part of achieving mission/business success in the threat environment of the 21st century.

An example of mission and business process reengineering related to risk management occurred recently within a prominent organization of the federal government. After a significant breach to one of the organization's most critical information systems, the authorizing official decided to disconnect the compromised system from the network. This unprecedented decision was based on a risk assessment of the information system including the system's environment of operation, the current information technology employed within the system, and the available security controls needed to protect the system. The ultimate risk to the organization's operations and assets, individuals, other organizations that it partners with, and the Nation, given the current state of technology, safeguards, and countermeasures, was deemed by the senior leadership to be too great, and the extraordinary measures were taken. The missions and business processes of the organization were reengineered in order to find new ways to carry out the traditional business functions of the organization that did not depend on certain information technologies and network connectivity.

CHAPTER THREE

THE PROCESS

APPLYING THE RISK MANAGEMENT FRAMEWORK

This chapter describes the process of managing risk to organizational missions and business functions that arises from the operation and use of information systems including: (i) conducting security categorizations to assess worst-case adverse impact as well as mission/business gains; (ii) selecting and tailoring initial sets of minimum (baseline) security controls as the starting point for providing adequate security;[40] (iii) supplementing the tailored security control baselines as necessary based upon organizational assessments of risk to achieve an agreed-upon level of risk mitigation for the particular environments of operation; (iv) documenting the resulting security controls in approved security plans for the information systems; (v) implementing the security controls using defense-in-depth and defense-in-breadth approaches; (vi) assessing implemented security controls for effectiveness; (vii) authorizing and reauthorizing the information systems for operation; and (viii) employing a comprehensive continuous monitoring process to effectively track the security state of the information system and the organization over time.

3.1 RISK MANAGEMENT FRAMEWORK

The NIST *Risk Management Framework* provides the organization with a disciplined, structured, flexible, extensible, and repeatable process for achieving risk-based protection related to the operation and use of information systems. While the risk framework is generally applied to information systems within an organization in a bottom-up (system-by-system) approach, the identification, development, and employment of common security controls (i.e., infrastructure-based security controls), the security categorization of information systems as an organization-wide activity, and the use of a risk executive function facilitates a top-down, organizational view of the information security program. The Risk Management Framework embodies a holistic approach to managing risk from information systems to organizational operations, organizational assets, individuals, other organizations, or the Nation based upon a comprehensive application of the framework steps to both information systems and the organization.

The Risk Management Framework can be applied to new and legacy information systems and operates within the context of the Federal Enterprise Architecture and the system development life cycle (see Appendix D). The framework represents an information security life cycle that facilitates continuous monitoring and continuous improvement in the security state of the information systems within the organization as well as the organization's information security program as a whole. The Risk Management Framework incorporates a well-defined set of information security standards and guidelines for federal agencies and support contractors to facilitate and demonstrate compliance with the FISMA legislation. The plug-and-play nature of the Risk Management Framework, however, allows other communities of interest (e.g., state, local, and tribal governments, private sector entities) to use the framework voluntarily either with the NIST security standards and guidelines or with industry-specific standards and guidelines. The Risk Management Framework provides organizations with the flexibility needed to apply the right security controls to the right information systems at the right time to adequately protect the critical missions and business functions of the organization.

[40] Tailoring guidance in NIST Special Publication 800-53 provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baselines.

The Risk Management Framework consists of eight steps that are paramount to the effective management of risk resulting from the operation and use of information systems. Figure 3 illustrates the steps in the framework and the NIST information security standards and guidelines associated with each step.

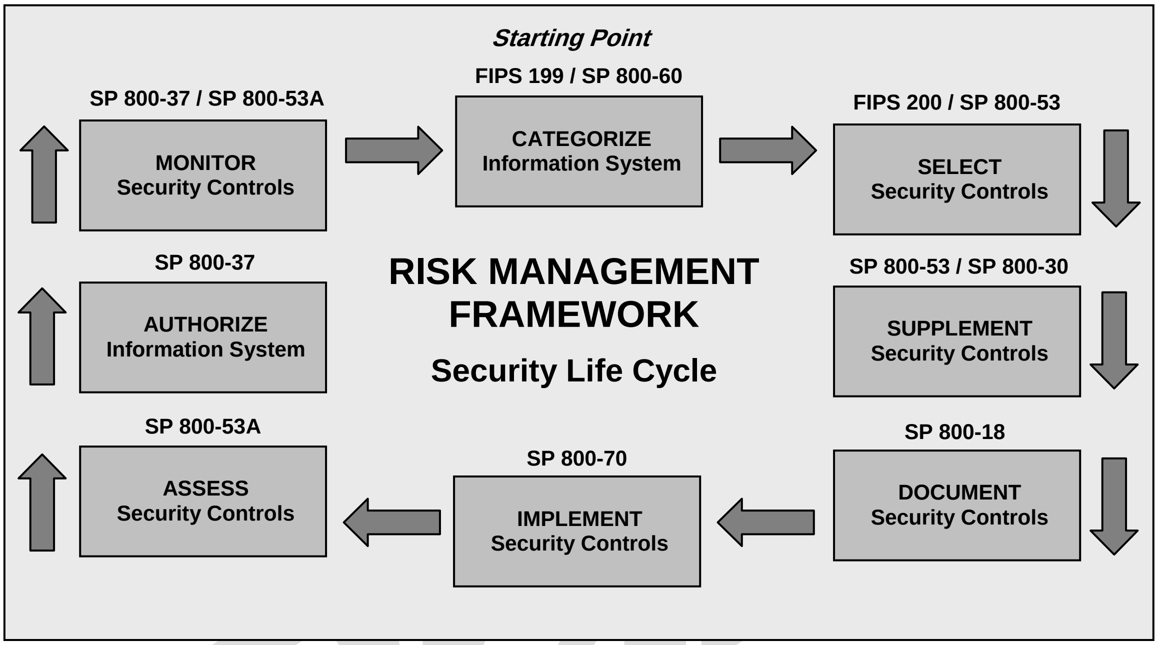

FIGURE 3: THE RISK MANAGEMENT FRAMEWORK

The following section describes how the Risk Management Framework can be applied to an information system and then extended to include organization-wide considerations to help ensure that the broad goals and objectives of the organization are met and that critical missions and business functions are adequately protected.

Risk Management Framework Steps

- Categorize the information system and the information resident within the system based on a FIPS 199 impact analysis[41] and the impact recommendations for the information types listed in NIST Special Publication 800-60.

  Organizational Application: *Conduct security categorizations as an organization-wide activity with the active participation of key senior leaders to help ensure the assessments (both potential value and adverse impacts) are as complete and accurate as possible, receive appropriate management oversight, and reflect the needs of the organization as a whole.*

- Select an initial set of security controls for the information system (i.e., baseline controls from NIST Special Publication 800-53) based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply the tailoring guidance, as appropriate, to obtain the control set used as the starting point for the risk assessment associated with the operation and use of the information system.

[41] The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system.

Organizational Application: *Select the initial security control baselines and identify common security controls as an organization-wide activity with the participation of key senior leaders to help ensure that the security program or infrastructure-related controls are assigned to appropriate entities within the organization and any organization-wide guidelines or restrictions on tailoring activities are disseminated and consistently applied across the organization.*

- Supplement the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific and credible threat information, cost-benefit analyses, or special circumstances.[42]

  Organizational Application: Provide organizational guidance to individual authorizing officials and information system owners regarding any additional security controls (including common controls supporting the infrastructure or information security program) that are considered generally needed to adequately mitigate risk and protect the organization's missions and business functions based on information received by or specific requirements of the organization. Also ensure that in the determination of risk being incurred, consideration is given to potential negative impacts not only to the missions and business functions supported by the information system, but also to the organization as a whole and to individuals, other organizations, and the Nation.

- Document the agreed-upon set of security controls in a system security plan approved by the appropriate authorizing official(s) including the organization's rationale for any refinements or adjustments to the initial set of controls.[43]

  Organizational Application: *Ensure that all security controls affecting the organization are: (i) documented either in the security plans for individual information systems or, in the case of common controls, by the organizational entities responsible for the development, implementation, and assessment of those controls; and (ii) that both the providers of common controls and the consumers of those controls are knowledgeable of any inheritance relationships Also ensure that the organizational risk executive function has visibility into individual system security plans as necessary to facilitate consistency of such plans and risk management decisions across the organization and the sharing of lessons learned and best practices.*

- Implement the security controls in the information system.

  Organizational Application: *Provide organizational guidance for the implementation of mandatory security configuration settings including configuration settings required by federal policy and local requirements, and disseminate to appropriate entities within the organization. Disseminate any other organization-level security control implementation information required to support the missions and business functions of the organization.*

- Assess the information system security controls for effectiveness using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[44]

  Organizational Application: *Provide organizational guidance on the conduct of security assessments to ensure that the assessments are consistent with the mission/business process needs of the organization. Ensure that the results of common security control assessments are distributed to information system owners inheriting those controls and that assessment results for individual information systems are shared across the organization when the results indicate systemic or organization-wide weaknesses or deficiencies.*

[42] NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (Initial Public Draft projected for publication in December 2007), provides guidance on applying risk assessments at various steps in the NIST Risk Management Framework.

[43] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

[44] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Third Public Draft), June 2007, provides guidance for determining the effectiveness of security controls.

- Authorize information system operation (with implemented security controls) based upon a determination of the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and an explicit decision to accept this risk.[45]

  Organizational Application: *Use the risk executive function to help ensure that broader, organizational perspectives are included in individual authorization decisions, to share authorization results from individual information systems with appropriate organizational officials, and to facilitate consistent authorization decisions across the organization; helping to ensure that the mission/business functions carried out by the organization are adequately protected and that the risks resulting from the operation and use of the information systems are considered among the other risks affecting the organization.*

- Monitor selected security controls in the information system[46] on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the system security status to appropriate organizational officials on a regular basis.[47]

  Organizational Application: *Provide organizational guidance and oversight to help ensure that the ongoing monitoring of the information system security controls is conducted consistently across the organization in accordance with mission/business priorities and any other relevant information provided by the organization. Ensure common security controls are monitored and the results shared among information system owners inheriting those controls.*

Figure 4 illustrates the information security activities that result from the application of the Risk Management Framework organization-wide.

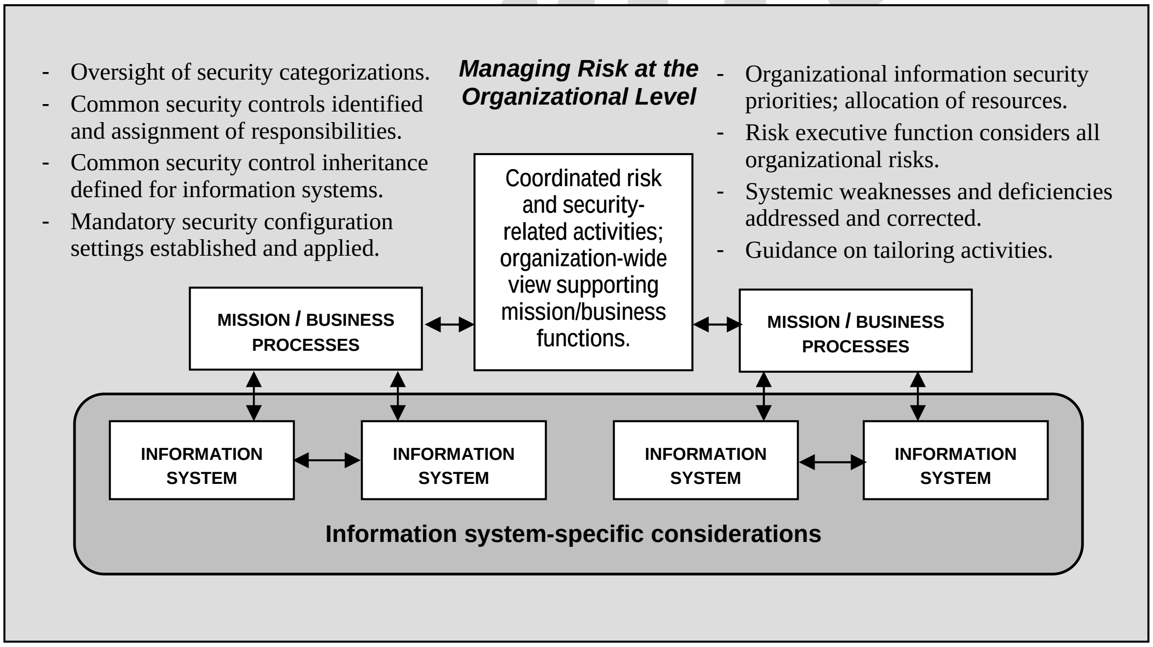
- Oversight of security categorizations.
- Common security controls identified and assignment of responsibilities.
- Common security control inheritance defined for information systems.
- Mandatory security configuration settings established and applied.
Managing Risk at the Organizational Level
- Organizational information security priorities; allocation of resources.
- Risk executive function considers all organizational risks.
- Systemic weaknesses and deficiencies addressed and corrected.
- Guidance on tailoring activities.
Coordinated risk and security-related activities; organization-wide view supporting mission/business functions.
MISSION / BUSINESS PROCESSES
MISSION / BUSINESS PROCESSES
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Information system-specific considerations

FIGURE 4: ORGANIZATION-WIDE VIEW OF SECURITY ACTIVITIES

[45] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization and reauthorization of information systems.

[46] Monitoring security controls in the information system includes monitoring of the environment in which the system operates. This occurs due to the breath of security control coverage from the families of controls in NIST Special Publication 800-53 which includes such areas as physical and environmental protection controls, personnel security controls, and media protection controls. This approach is consistent with the broad definition of an information system which is taken to include people, processes, and technologies.

[47] Continuous monitoring includes tracking and updating the plans of action and milestones documents.

3.2 SECURITY CATEGORIZATION

Security categorization is the first and arguably the most important step in the Risk Management Framework. Security categorization employs FIPS 199 and NIST Special Publication 800-60 to determine the criticality and sensitivity of the information system and the information being processed, stored, and transmitted by the system. FIPS 199, the security categorization standard, is predicated on a simple and well-established concept—determining priorities for organizational information systems and subsequently applying appropriate measures to adequately protect the organizational missions and business functions supported by those systems. The security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, individuals, other organizations, or the Nation, should there be a loss of confidentiality, integrity, or availability.[48] FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems.[49] The generalized format for expressing the security category (SC) of an information system is:

$$\textbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of prioritizing information security efforts among information systems and selecting an initial set of security controls from one of the three security control baselines.[50] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high. As indicated above, the high water mark provides an initial entry point into the NIST process for selecting the appropriate security controls for the information system. Also, by stating the maximum potential impact on the organization, the high water mark provides an effective security categorization for information system priority within the organization's information security program.[51]

[48] NIST Special Publication 800-53 (security control RA-2, *Security Categorization*) extends the language in FIPS 199 in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, to include consideration of potential national-level impacts and impacts to other organizations.

[49] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

[50] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective; rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The tailoring guidance in NIST Special Publication 800-53 provides for selective security control baseline adjustments based upon the individual impact levels for confidentiality, integrity, and availability. These tailoring adjustments to the initial security control baselines ensure that the use of the high water mark does not result in an over specification of security controls for information systems.

[51] Note, however, that while the *high water mark* facilitates information system prioritization, the separate impact level determinations for confidentiality, integrity, and availability remain and are used subsequently in both risk assessments and the NIST Special Publication 800-53 security control selection process (both in tailoring the initial set of baseline controls and in supplementing the controls) to ensure adequate security.

Organizations should conduct FIPS 199 security categorizations as an organization-wide activity with the involvement of the senior leadership and other key officials within the organization (e.g., mission and business owners, authorizing officials, risk executive, chief information officer, senior agency information security officer, information system owners, and information owners). Conducting the security categorization activity as an organization-wide exercise helps ensure that the categorization process accurately reflects the actual criticality, sensitivity, and priority of the information systems with respect to supporting organizational missions and business functions. Senior leadership oversight in the security categorization process is essential so that the next steps in the Risk Management Framework can be carried out in an effective manner. A mistake in the initial security categorization process can result in either an over specification or under specification of security controls for organizational information systems. Over specification of security controls means that the organization is spending more on information security than is actually necessary and potentially taking resources away from other information systems with greater mission and business process protection needs. Under specification of security controls means that selected missions and business functions may be at greater risk due to the insufficient safeguards and countermeasures defined for the information systems involved. FIPS 199 security categories should be reviewed on an ongoing basis to help ensure that impact assessments reflect the current organizational environment and priorities.

3.3 SECURITY CONTROL SELECTION

Security control selection is the second step in the Risk Management Framework and employs FIPS 200 and NIST Special Publication 800-53 to determine the needed security controls for the information system.[52] Once the security categorization of the information system is determined in accordance with FIPS 199, minimum security requirements are established by FIPS 200 and an initial set of security controls can be selected from the corresponding low, moderate, or high baselines listed in NIST Special Publication 800-53. Organizations have the flexibility to *tailor* the security control baselines in accordance with the terms and conditions set forth in Special Publication 800-53. Tailoring guidance facilitates customization of security controls in the initial baselines to more closely meet the protection needs of the organization. Tailoring activities include: (i) the application of appropriate scoping guidance to the initial security control baselines; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in selected security controls, where allowed.

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines from NIST Special Publication 800-53. The scoping guidance allows organizations to shape or fine-tune the security controls in the initial baselines, considering such factors as common security controls;[53] adjustments in impact levels for security objectives; technologies employed; operational and environmental conditions; the layout of facilities and physical infrastructure; public access requirements; scalability; and applicable laws, Executive Orders, directives, policies, standards, or regulations. Certain scoping activities should be conducted from an organization-wide perspective. For example, the identification of common security controls should occur only with the involvement of the senior leadership of the organization. Scoping decisions should be documented in the information system security plans.

[52] Security control selection is the first of two steps in deciding upon the degree of risk mitigation required to protect an organization's missions and business functions and the information systems that support those missions and functions. The second step, supplementation, completes the risk mitigation determination process.

[53] Common security controls are controls that can be applied to one or more organizational information systems. The responsibility for the development, implementation, and assessment of common security controls resides with the organization, not with the individual information system owners.

With the diverse nature of information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. Compensating security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended security controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for information systems. Compensating controls for information systems may be employed by an organization only under the following conditions: (i) the organization selects the compensating controls from NIST Special Publication 800-53 or, if appropriate compensating controls are not available in the security control catalog, the organization adopts suitable compensating controls; (ii) the organization provides a complete and convincing rationale[54] for how the compensating controls provide an equivalent security capability or level of protection for the information systems and why the related baseline security controls could not be employed; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating controls in the information systems. The use of compensating controls should be documented in the system security plans and approved by the respective authorizing officials.

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. After the application of the scoping guidance and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. Organization-defined security control parameters should be documented in the information system security plans.

3.4 SECURITY CONTROL SUPPLEMENTATION

Security control supplementation is the third step in the Risk Management Framework and employs NIST Special Publications 800-30 and 800-53 to determine the need for additional security controls for the information system. The tailored security control baselines should be viewed as the foundation or starting point in the selection of adequate security controls for information systems necessary to protect organizational missions and business functions. The tailored baselines represent, for particular security categories of information systems (derived from the FIPS 199 impact analyses and modified appropriately for local conditions), the starting point for determining the needed level of *security due diligence* to be demonstrated by an organization. The final determination of the appropriate security controls necessary to provide adequate security is a function of the organization's assessment of risk and the information system trustworthiness (see Section 2.3) required to sufficiently mitigate organizational risks. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in information systems or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baselines—that is, the security controls needed to adequately protect organizational operations, organizational assets, individuals, other organizations, and the Nation.

[54] Throughout the Risk Management Framework, the meaning for terms such as convincing, complete, and sound for a rationale is determined with regard to the level of potential impact that can occur, with lower impact systems requiring less rigorous rationale than higher impact systems.

There may be situations in which an organization discovers that it is employing information technologies beyond its ability to adequately reduce or mitigate risks to organizational missions and business functions from the operation and use of information systems. In those situations, an alternative strategy is needed to protect the organization, a strategy that considers the risks that are being brought about by an aggressive use of information technology. Information system use restrictions provide an alternative method to reduce or mitigate risk when: (i) security controls cannot be implemented within technology and resource constraints; or (ii) security controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of an information system are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined and sophisticated adversaries. The final determination of required information system use restrictions should be made by the appropriate organizational officials responsible for managing risk. These officials typically include, mission and business owners, information system owners, authorizing officials, senior agency information security officers, and chief information officers. Examples of use restrictions include: (i) limiting either the information a system can process, store, or transmit or the manner in which a mission or business process is automated; (ii) prohibiting external information system access to critical organizational information by removing selected system components from the network (i.e., air gapping); and (iii) prohibiting moderate- or high-impact information on information system components to which the public has access, unless an explicit determination is made authorizing such access. Figure 5 summarizes the security control selection and supplementation processes.[55]

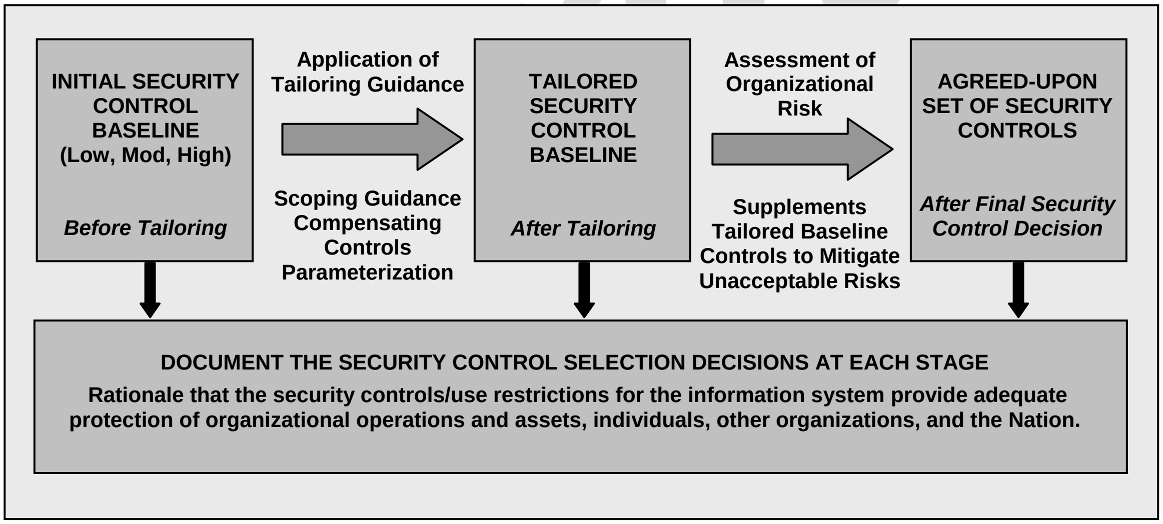
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to Mitigate Unacceptable Risks
AGREED-UPON SET OF SECURITY CONTROLS
After Final Security Control Decision
DOCUMENT THE SECURITY CONTROL SELECTION DECISIONS AT EACH STAGE
Rationale that the security controls/use restrictions for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

FIGURE 5: SECURITY CONTROL SELECTION AND SUPPLEMENTATION

[55] Organizations are encouraged to make maximum use of NIST Special Publication 800-53 to facilitate the process of enhancing security controls or adding controls to the tailored baselines. To assist in this process, the security control catalog contains numerous controls and control enhancements that are found only in higher-impact baselines or are not included in any of the baselines.

3.5 SECURITY CONTROL DOCUMENTATION

Security control documentation is the fourth step in the Risk Management Framework and employs NIST Special Publication 800-18 to guide the content of security plans for information systems. It is important for organizations to document the decisions taken during the initial security control selection, tailoring, and the supplementation process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for information systems with respect to potential mission or business impact. The resulting set of security controls along with the supporting rationale for control selection decisions and any information system use restrictions are documented in the security plans for the information systems. This provides a clear description of the *risk mitigation* deemed necessary, and the information system *trustworthiness* thereby required, in order to adequately ensure mission accomplishment and success of business functions potentially impacted by the operation and use of the systems. Security plans are also used to organize and manage the security activities for information systems, organization-wide. Security plans provide a road map for how an organization intends to protect the information systems that support organizational missions and business functions. Security plans provide an overview of the security requirements for the information systems within the organization and describe the security controls in place or planned for meeting those requirements.[56] In addition, the security plans for organizational information systems describe how individual security controls are implemented within specific operational environments. And finally, security plans provide the rationale for decisions taken by the organization in tailoring and supplementing the baseline security controls during the selection and supplementation steps in the Risk Management Framework. The agreed-upon security controls should be documented in the information system security plans.

In addition to the security plans developed for information systems, there are organizational responsibilities to provide documentation for security controls that serve the organization at large. Organizations should document all designated common security controls to ensure that the controls are effectively managed. Common security controls can support multiple information systems across the organization and can have widespread effects if such controls are not properly developed, implemented, and assessed for effectiveness. Providing appropriate documentation for common security controls ensures that appropriate officials take responsibility for the development, implementation, and assessment of these controls. It is also important that as the common controls are implemented, the results of the activities associated with the common control development, implementation, and assessment are conveyed to the information system owners and authorizing officials that depend upon those common controls (through inheritance) to help protect the missions and business functions supported by their systems.

The organization-wide approach for security control documentation ensures that risks to missions and business functions are adequately mitigated and all security controls required by the organization, whether system-specific, hybrid, or common, are either contained within some information system security plan or documented in some other manner by the organization. Complete coverage of security controls in appropriate security plans facilitates more comprehensive information security, promotes increased accountability, and provides an effective vehicle for organizational officials to better manage the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation or use of information systems.

[56] Security plans for information systems should also reference any common security controls that have been identified by the organization and assigned to other organizational entities for development, implementation, and assessment.

3.6 SECURITY CONTROL IMPLEMENTATION

Security control implementation is the fifth step in the Risk Management Framework and employs enterprise architectures, the system development life cycle, and NIST Special Publication 800-70 to guide the implementation of security controls in organizational information systems. Security controls that are documented in information system security plans are allocated to specific information resources (including people, processes, and technologies). This requires a determination by knowledgeable individuals within the organization (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists, etc.) as to which personnel, processes, hardware, software, firmware, or environmental components within the system boundary are providing specific security functionality (e.g., access control, identification and authentication, auditing and accountability, system and communications protection, physical security, personnel security, incident response, contingency planning, etc.). There should be close coordination and collaboration among organizational personnel to ensure that the needed security functions are allocated to the appropriate resources within the information system. For common security controls, the organization should allocate those controls to organizational entities responsible for development, implementation, and assessment. For all required controls, the implementation should meet the trustworthiness requirements identified to provide the necessary functionality with sufficient quality and the assurance that this functionality and quality is being achieved (see Section 2.3),

Allocation of security controls and the associated security functions to the appropriate resources within information systems is a critically important activity that can affect the security posture of the organization. Information generated from the allocation of security controls to information system resources and how the controls are implemented should be documented in system security plans as described in the fourth step in the Risk Management Framework. Allocation decisions also affect the security assessments of information systems, informing assessors of system resources providing specific security capabilities.

Certain security controls employed within organizational information systems require that security configuration settings be established during implementation. Organizations are required to define mandatory configuration settings for all information technology products that are used within organizational information systems. The mandatory configuration settings should be enforced across the organization including all information systems that are supporting missions and business functions.[57] NIST Special Publication 800-53 identifies specific security controls where security configuration settings may be required. There are several efforts under way to standardize the security configuration settings for commercial information technology products and to use automated tools to determine if the required settings are in effect and providing the functionality required by the associated security controls.[58]

[57] OMB has established mandatory requirements for configuration settings (i.e., Federal Desktop Core Configurations) for selected information technologies. Organizations can comply with OMB policy and, at the same time, maintain a diversity of information technology assets within the organization in accordance with the strategic considerations described in Section 2.5. The standardized configuration settings apply to the specific information technology products that the organization chooses to deploy and for which mandatory configuration settings have been defined. The policy does not constrain the types of information technology products organizations can employ in their information systems.

[58] To facilitate more cost-effective and comprehensive security with regard to configuration settings for information technology products, NIST has initiated the Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP). The primary purpose of the SCAP is to improve the automated application, verification, and reporting of commercial information technology product-specific security configuration settings, thereby reducing vulnerabilities when products are not configured properly.

3.7 SECURITY CONTROL ASSESSMENT

Security control assessment is the sixth step in the Risk Management Framework and employs NIST Special Publication 800-53A to determine the effectiveness of security controls within the information system, that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in an information system is essential in determining the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of the system. Security assessments are, in essence, the compilation of the evidence necessary to provide the required assurance that intended information system functionality has been achieved with the requisite level of quality—that is, the system possesses the agreed-upon level of trustworthiness. These assessments, therefore, promote a better understanding of risks from information systems and create more complete, reliable, and trustworthy information for organizational officials to support information sharing activities, authorization decisions,[59] and FISMA compliance.

Organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available on information system components from independent, third-party testing, evaluation, and validation activities. Product testing, evaluation, and validation are routinely conducted today on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, web browsers, web applications, smart cards, biometrics devices, personal identity verification devices, web applications, network devices, and hardware platforms using national and international standards. These types of product assessments provide a more in-depth examination of the security features provided by the products at a level of depth and rigor that is not practical in most information system assessments.

Assessors obtain the evidence needed during the assessment process to allow the appropriate organizational officials to make objective determinations about the effectiveness of the security controls and the security of the information system. The assessment evidence needed to make such determinations can be obtained from a variety of sources including, but not limited to, information technology product and system assessments. Product assessments (also known as product testing and evaluation) are typically conducted by independent, third-party testing organizations and examine the security functions of products and established configuration settings. Assessments can be conducted against industry, national, and international information security standards as well as developer and vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in thousands of information systems, these types of assessments may provide a cost-effective method for obtaining the necessary assurances regarding security functionality and quality.

System assessments are typically conducted by information system developers, integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs of organizations. These assessors or assessment teams bring together available information about the information system such as the results from product assessments, if available, and conduct additional system assessments using a variety of methods and techniques.

[59] NIST Special Publication 800-37 provides guidance on information system authorization decisions and the acceptance of mission/business process risk. The publication also provides guidance on the security certification process, a process that determines the effectiveness of security controls in organizational information systems in support of the authorization process.

System assessments are used to compile and evaluate the evidence needed by organizational officials to determine how effective the security controls employed in an information system are likely to be in achieving the intended mitigation of risks to organizational operations, organizational assets, individuals, other organizations, and the Nation. The results from assessments conducted using assessment procedures derived from the guidelines in NIST Special Publication 800-53A contribute to compiling the necessary evidence to determine security control effectiveness in accordance with the assurance requirements in NIST Special Publication 800-53.

Security assessments should be conducted on security controls within organizational information systems and also on common security controls identified by the organization. For assessments on common security controls, the evidence regarding control effectiveness should be conveyed to all information system owners and authorizing officials that depend on those controls (through inheritance) for the protection of organizational missions and business functions.

3.8 INFORMATION SYSTEM AUTHORIZATION

Information system authorization is the seventh step in the Risk Management Framework and employs NIST Special Publication 800-37 to guide the activities related to the decision to authorize the operation of an information system or continue its operation and to explicitly accept the resulting risks to organizational operations, organizational assets, individuals, other organizations, or the Nation. The authorization decision is one of the most important decisions made by an authorizing official. With the move toward risk-based protection, authorizing officials, more than ever before, must take ownership of the potential risks to organizational missions and business functions due to the use of information systems, as well as the operational gains such systems make possible. As part of this, authorizing officials must take ownership of the security plans developed for their information systems that define the risk mitigation needed, providing the level of system trustworthiness, to include identification of the appropriate safeguards and countermeasures agreed upon as necessary and sufficient to protect the organizational missions and business functions. While there is great flexibility in developing the right set of safeguards and countermeasures for appropriately managing organizational risk, there is also great responsibility and accountability for the decisions made by authorizing officials in exercising this flexibility to specify acceptable security solutions. In explicitly understanding and accepting the risk resulting from their authorization decisions, they assume the responsibility and accountability for these decisions.

Authorization decisions should also consider organizational risks brought about by the use of external providers of services and information (e.g., outsourcing, service-oriented architectures, software as a service, lines of business, etc.) in customer/provider relationships and peer-to-peer relationships where organizations partner in the accomplishment of missions and business functions. Such relationships require the establishment of trust among participating/cooperating organizations. The trust relationships are based on the trustworthiness of the information systems providing the services or information to include the evidence brought forth by the external providers demonstrating that functionality and quality claims are being met. The degree of trustworthiness of the information systems employed by external providers should be factored into the authorization decisions and explicit acceptance of risk by authorization officials. Finally, authorization decisions by senior leaders can no longer be made in isolation and instead need to be made with regard to organization-wide missions and business process considerations. Making information security a part of the risk executive function helps ensure that the strategic goals and objectives of the organization are always taken into account when considering the individual authorization (risk acceptance) decisions for organizational information systems.

3.9 CONTINUOUS MONITORING

Security control monitoring is the final step in the Risk Management Framework and employs NIST Special Publications 800-37 and 800-53A to determine the ongoing effectiveness of security controls in organizational information systems and using the resulting information on the security state to manage organizational risk. Conducting a thorough point-in-time assessment of the security controls in an organizational information system is a necessary but not sufficient condition to demonstrate security due diligence. Effective information security programs should also include an aggressive continuous monitoring program to check the status of the security controls in the information system on an ongoing basis. The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates.

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials.[60] This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results from that decision. Continuous monitoring programs provide organizations with an effective tool for producing ongoing updates to information system security plans, security assessment reports, and plans of action and milestones documents.[61] An effective organization-wide continuous monitoring program requires:

- Configuration management and control processes for organizational information systems;
- Security impact analyses of changes to the organization's information systems;[62]
- Assessment of selected security controls in the information systems; and
- Security status reporting to appropriate organizational officials.

Organizations should use the current risk assessment, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process. Priority for control monitoring should be given to the security controls that have the greatest volatility (i.e., greatest potential for change) after implementation and the controls that have been identified in the organization's plan of actions and milestones document for the information system. Security control volatility is a measure of how frequently a control is likely to change over time. For example, security policies and implementing procedures in a particular organization are less likely change from one year to the next and thus would be a security control with lower volatility. Access control mechanisms or other technical controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of an information system would therefore be security controls with higher volatility. Organizations should apply greater resources to security controls deemed to be of higher volatility as there is typically a higher return on investment for

[60] NIST Special Publication 800-37 provides guidance on the security certification and accreditation process in general and on the continuous monitoring process in particular.

[61] Organizations can use the current year's assessment results obtained during the continuous monitoring process to meet the annual FISMA assessment requirements.

[62] Changes to information systems include security-related aspects of the operational environment.

assessing security controls of this type. Security controls identified in the plan of actions and milestones document should also be a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree (or nonexistent, in the worst case).

Since organizations operate in dynamic environments with constantly changing threats, vulnerabilities, and technologies, authorization decisions and the risk acceptance associated with those decisions, need to be revisited on a regular basis. Risk-based protection approaches are redefining how organizations conduct certification and accreditation processes and the results produced from those processes. Certification and accreditation processes are explicitly reflected in the NIST Risk Management Framework[63] with the first five steps in the framework corresponding to the Initiation Phase, and the sixth, seventh, and eighth steps corresponding to the Certification, Accreditation, and Continuous Monitoring Phases, respectively.[64] The ability to update authorization decisions in near real-time to get an accurate picture of the current security state of an organization's information systems is paramount to effectively managing risk. The employment of automated support tools to allow authorizing officials to obtain frequent security status information by examining the security plans for information systems, updated risk assessments, security assessment reports, and the plans of action and milestones documents, is critical to understanding and explicitly accepting risk on a day-to-day basis.

In summary, organizations must make informed judgments regarding the application of limited assessment resources when conducting continuous monitoring activities to ensure that the expenditures are consistent with the organization's mission requirements, security categorization in accordance with FIPS 199, and testing requirements articulated in federal legislation, policy, directives, and regulations. As the security certification and accreditation process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the system development life cycle, the ability to update the security assessment report frequently based on the assessment results obtained from the continuous monitoring process becomes a critical aspect of an organization's information security program. It is important to emphasize the relationship, described in NIST Special Publication 800-37, among the three key documents in the information system authorization package (i.e., the system security plan including the organizational assessment of risk, the security assessment report, and the plan of action and milestones). It is these documents that provide the best indication of the overall security status of the information system and the ability of the system to adequately protect, to the degree necessary, the missions and business functions of the organization. Updates to these key documents should be provided on an ongoing basis in accordance with the continuous monitoring program established by the organization.

[63] Certification and accreditation processes should operate within the system development life cycles of organizational information systems. The execution of the Risk Management Framework helps ensure that information system certification and accreditation processes (resulting in authorization decisions) remain tightly coupled to the system development life cycle processes, thus becoming part of managing risk resulting from the operation and use of information systems.

[64] NIST Special Publication 800-37 provides guidance on executing the four phases of the security certification and accreditation process.

Mission First Philosophy

Above all, information security is a mission and business enabler with respect to reliability, fidelity, and quality. Information security should never impede or detract from the conduct or successful completion of organizational missions and business processes. In short, mission and business success demands ownership of the risks as well as the rewards.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES[65]

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.

POLICIES, DIRECTIVES, INSTRUCTIONS, REGULATIONS, AND MEMORANDA

6. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
7. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
8. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

STANDARDS

9. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
10. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

GUIDELINES

11. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
12. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. (Note: This document is currently under revision and will be reissued as Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.)
13. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
14. National Institute of Standards and Technology Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

[65] The status of and most current versions of NIST publications including FIPS and Special Publications in the 800-series (draft and final) can be found at http://csrc.nist.gov/publications.

15. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Third Public Draft), June 2007.

16. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

17. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

18. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

19. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

20. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

21. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, February 2007.

22. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

MISCELLANEOUS PUBLICATIONS

23. *The Federal Enterprise Architecture Security and Privacy Profile*, v2.0, June 2006.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-39. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation
[FIPS 200, NIST SP 800-37]
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Accreditation Boundary
[NIST SP 800-37]
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

Accrediting Authority
See Authorizing Official.

Adequate Security
[OMB Circular A-130, Appendix III]
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency
See Executive Agency.

Authentication
[FIPS 200]
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticity
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorize Processing
See Accreditation.

Authorizing Official
[FIPS 200, NIST SP 800-37]
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Availability
[44 U.S.C., Sec. 3542]
Ensuring timely and reliable access to and use of information.

Boundary Protection
Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.

Certification
[FIPS 200, NIST SP 800-37]

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certification Agent
[NIST SP 800-37]

The individual, group, or organization responsible for conducting a security certification.

Chief Information Officer
[PL 104-106, Sec. 5125(b)]

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Classified National Security Information
[E.O. 13292]

Information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Common Security Control
[NIST SP 800-37]

Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compensating Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

Confidentiality
[44 U.S.C., Sec. 3542]

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control
[CNSS Inst. 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Countermeasures
[CNSS Inst. 4009]

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Executive Agency
[41 U.S.C., Sec. 403]

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External Information System (or Component)

An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service

An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).

External Information System Service Provider

A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges (i.e., supply chain collaborations or partnerships).

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
[40 U.S.C., Sec. 11331]

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

High-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Hybrid Security Control

Security control that has the properties of both a common security control and a system-specific security control (i.e., one part of the control is deemed to be common, while another part of the control is deemed to be system-specific).

Incident
[FIPS 200]

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Industrial Control System

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information
[FIPS 199]

An instance of an information type.

Information Owner
[CNSS Inst. 4009]

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources
[44 U.S.C., Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy
[CNSS Inst. 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System
[44 U.S.C., Sec. 3502]
[OMB Circular A-130, Appendix III]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems consist of people, processes, and technology.]

Information System Owner (or Program Manager)
[CNSS Inst. 4009, Adapted]

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer
[CNSS Inst. 4009, Adapted]

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Information Technology [40 U.S.C., Sec. 1401]

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type [FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity [44 U.S.C., Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Line of Business

The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.

Low-Impact System [FIPS 200]

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Malicious Code [CNSS Inst. 4009] [NIST SP 800-61]

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Management Controls [FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Media [FIPS 200]

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Sanitization [NIST SP 800-88]

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Moderate-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

National Security System
[44 U.S.C., Sec. 3542]

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation
[CNSS Inst. 4009 Adapted]

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Operational Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Organization
[FIPS 200]

A federal agency or, as appropriate, any of its operational elements.

Plan of Action and Milestones
[OMB Memorandum 02-01]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact
[FIPS 199 Adapted]

The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Risk
[FIPS 200 Adapted]

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment
[NIST SP 800-30, Adapted]

The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in-place security controls.

Risk Management
[FIPS 200 Adapted]

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation or use of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Safeguards
[CNSS Inst. 4009, Adapted]

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Scoping Guidance

Provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Category
[FIPS 199 Adapted]

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Security Controls
[FIPS 199]

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline
[FIPS 200]

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements

Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Security Functions

The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Impact Analysis
[NIST SP 800-37]

The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

Security Incident

See Incident.

Security Objective
[FIPS 199]

Confidentiality, integrity, or availability.

Security Perimeter

See Accreditation Boundary.

Security Plan

See System Security Plan.

Security Requirements
[FIPS 200]

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior Agency Information Security Officer
[44 U.S.C., Sec. 3544]

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

System

See Information System.

System-specific Security Control
[NIST SP 800-37]

A security control for an information system that has not been designated as a common security control.

System Security Plan
[NIST SP 800-18, Rev 1]

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Tailoring

The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

Tailored Security Control Baseline

Set of security controls resulting from the application of the tailoring guidance to the security control baseline.

Technical Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source
[FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

User
[CNSS Inst. 4009]

Individual or (system) process authorized to access an information system.

Vulnerability
[CNSS Inst. 4009, Adapted]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
DCID	Director of Central Intelligence Directive
DOD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication

APPENDIX D

MANAGING RISKS WITHIN LIFE CYCLE PROCESSES

APPLYING THE RISK MANAGEMENT FRAMEWORK WITHIN THE SDLC

Managing the risks from information systems includes addressing the causes of vulnerabilities that arise during the design, development, implementation, operation, and disposition of information systems. This should be accomplished in the context of the routine system development life cycle (SDLC) processes employed by organizations. Information security considerations should be addressed by organizations as early as possible in the SDLC process to ensure the most cost-effective implementation of the safeguards and countermeasures needed to adequately mitigate risk from the operation and use of information systems. Each phase of the SDLC includes a minimum set of information security-related activities required to effectively incorporate security capabilities into information systems.[66] The steps in the NIST Risk Management Framework (RMF) are addressed within the security activities described for the SDLC. The Risk Management Framework can be applied to both new development systems and legacy systems. Table D-1 illustrates the security activities and Risk Management Framework steps that are applied at each phase of the SDLC.

TABLE D-1. SECURITY ACTIVITIES INTEGRATED INTO THE SDLC PROCESS

SDLC PHASE	Security Activities and RMF Steps
Initiation	*Needs Determination* *Preliminary Risk Assessment* *Security Categorization—**Step 1 RMF***
Development and Acquisition	*Requirements Analysis* *Risk Assessment* *Cost Considerations and Reporting* *Security Planning* - *Security Control Selection and Tailoring—**Step 2 RMF*** - *Security Control Supplementation—**Step 3 RMF*** - *Security Control Documentation—**Step 4 RMF*** *Security Control Development**—Step 5 RMF*** *Developmental Security Test and Evaluation**—Step 5 RMF*** *Other Planning Components*
Implementation	*Inspection and Acceptance* *System Integration—**Step 5 RMF*** *Security Certification—**Step 6 RMF*** *Security Accreditation—**Step 7 RMF***
Operations and Maintenance	*Configuration Management and Control* *Continuous Monitoring—**Step 8 RMF***
Disposition	*Information Preservation* *Media Sanitization* *Hardware and Software Disposal*

[66] NIST Special Publication 800-64 presents a framework for incorporating information security into all phases of the SDLC to ensure the selection, acquisition, and use of appropriate and cost-effective security controls.

In many cases, organizations will be applying information security to legacy information systems that have been in operation for some extended period of time with a set of security controls already in place. Some legacy systems may have excellent security plans that provide comprehensive documentation of the risk management decisions that have been made, to include identifying the security controls currently employed. However, other systems may have little, if any, documentation available. For legacy information systems, although the system is in the operations and maintenance phase of the SDLC, the Risk Management Framework still applies and can be thought of as a potential system upgrade that represents a full SDLC from requirements identification and necessary development/acquisition to implementation of the upgrade and back into operations and maintenance. The first four steps in the Risk Management Framework are executed and culminate in the development of an agreed-upon set of security controls for the information system.

At this point in the process, the agreed-upon security controls are compared to the actual controls that have been employed in the legacy system to determine if there are any discrepancies or shortfalls. The delta factor, or difference between the actual security controls employed in the legacy information system versus the controls necessary to adequately protect the organizational missions and business functions supported by the system, provides the necessary information to initiate appropriate upgrades. If a security plan exists, it is updated with the additional security controls and/or control enhancements identified during the execution of the initial steps in the Risk Management Framework. If a security plan does not exist, a plan is created, documenting the agreed-upon security controls. Next, the necessary acquisitions and development activities are carried out to implement these controls. Once the additional security controls have been implemented, completing the fifth step in the Risk Management Framework, the final three steps can be initiated resulting in the assessment of the security controls, the authorization decision, and continuous monitoring of the legacy system.

Table D-2 is intended to assist system developers to better understand the relationship between the acquisition cycle and the five basic steps of the SDLC.[67]

TABLE D-2. RELATIONSHIP OF ACQUISITION AND SDLC PHASES

<table>
<tr><th colspan="8">ACQUISITION CYCLE PHASES</th></tr>
<tr><td>Mission and Business Planning</td><td colspan="2">Acquisition Planning</td><td>Acquisition</td><td colspan="3">Contract Performance</td><td>Disposal and Contract Closeout</td></tr>
<tr><td colspan="2">Initiation</td><td colspan="3">Acquisition and Development</td><td>Implementation</td><td>Operation and Maintenance</td><td>Disposition</td></tr>
<tr><th colspan="8">SYSTEM DEVELOPMENT LIFE CYCLE PHASES</th></tr>
</table>

[67] General Services Administration publication, *A Guide to Planning, Acquiring, and Managing Information Technology Systems*, December 1998.

For both new development and legacy information systems, cost, schedule, and performance issues are the primary consideration for organizational officials concerned with carrying out critical missions and business functions. If information security requirements have been given a high priority by senior leaders and integrated into the SDLC process, then the safeguards and countermeasures needed to protect organizational operations, organizational assets, individuals, other organizations, or the Nation will have been included in the performance requirements for the information systems. Authorization decisions rendered for information systems include all relevant considerations in managing risk to ensure that the organization can effectively carry out its missions and business functions.

APPENDIX E

RISK MANAGEMENT APPROACHES

LINKING RISK MANAGEMENT FRAMEWORKS TO SUPPORT CRITICAL INFRASTUCTURES

The purpose of this section is to provide a mapping from the framework for managing risk described in the National Infrastructure Protection Plan (NIPP) and the NIST Risk Management Framework (RMF). These frameworks, while operating at different levels of abstraction, are complementary in nature and provide different perspectives on the same overall process. The NIPP framework for managing risk includes the following activities:

- Set security goals;
- Identify assets, systems, networks, and functions;
- Assess risks;
- Prioritize;
- Implement protective programs; and
- Measure effectiveness.

The activities in the NIPP framework for managing risk are described in greater detail below. A description of the closest corresponding step or steps from the NIST Risk Management Framework is provided for each NIPP framework activity. Note that since the respective frameworks are defined at different levels of abstraction, although there is good alignment between the frameworks, there is still overlap between NIPP framework activities and NIST RMF steps.

NIPP Framework Activity [Set security goals]: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.

NIST RMF Step [Security categorization]

NIPP Framework Activity [Identify assets, systems, networks, and functions]: Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation’s CI/KR and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

NIST RMF Step [Security categorization]

NIPP Framework Activity [Assess risks]: Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.

NIST RMF Steps [Security categorization, security control selection, supplementation]

NIPP Framework Activity [Prioritize]: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.

NIST RMF Steps [Security control selection, supplementation, documentation]

NIPP Framework Activity [Implement protective programs]: Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.

NIST RMF Step [Security control implementation]

NIPP Framework Activity [Measure effectiveness]: Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

NIST RMF Steps [Security control assessment, system authorization, security control monitoring]